(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
15 May 2003 (15.05.2003)

PCT

(10) International Publication Number
WO 03/040854 A2

(51) International Patent Classification[7]: G06F

(21) International Application Number: PCT/HR02/00048

(22) International Filing Date: 11 October 2002 (11.10.2002)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
P20010751A 17 October 2001 (17.10.2001) HR

(71) Applicant and
(72) Inventor: STIPCEVIC, Mario [HR/HR]; Ul. grada Chicaga 23, 10000 Zagreb (HR).

(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZM, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Declaration under Rule 4.17:
— *as to the identity of the inventor (Rule 4.17(i)) for all designations*

Published:
— *without international search report and to be republished upon receipt of that report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

WO 03/040854 A2

(54) Title: APPARATUS AND METHOD FOR GENERATING COMPLETELY RANDOM BITS BASED ON TIME SUMMATION OF AN ELECTRONICS NOISE SOURCE

(57) Abstract: An electronics device and associated method use an electronics noise source for production of truly random sequence of bits with a very small bias. The bias is defined as a difference between probability that a generator produce a high logical level bit and the ideal value of 0.5.The electronics noise source may, for example, be realized with a semiconductor Zener diode. The electronics noise source is AC coupled to a comparator with a self-regulating bias which ensures roughly equal probability of low and high states at the output of the comparator. The output of the said comparator is filtered through a stage composed of one JK flip-flop followed by an edge-triggered D flip-flop. This double flip-flop stage eliminates statistical bias and delivers a bit upon a request. A partial mathematical proof is presented which shows that that this generator, in the limit of low enough sampling rate, produces truly random bits. Complete proof can be found elsewhere (Stipcevic).If needed, a number of bits that are sequentially read form the generator can be grouped together to form random integer or real numbers.

APPARATUS AND METHOD FOR GENERATING COMPLETELY RANDOM BITS BASED ON TIME SUMMATION OF AN ELECTRONICS NOISE SOURCE

DESCRIPTION OF INVENTION

1 FIELD OF INVENTION

Present invention relates to apparatus and method for generating completely random bits (or numbers) based on the summation of time intervals produced by an electronics noise source.

According to the international IPC classification, the invention is classified as: **G 06 F 7/58**.

2 TECHNICAL PROBLEM

Hardware generators of random bits (or numbers) are used a lot in different areas: ingeniering, technology, science, hazard games, cryptography etc. Hardware generators are characterized by the fact that their output can not be predicted, just as it would be impossible to predict outcome of flipping a fair coin. Main problem, however, is to construct a good enough generator, whose output can be for all practical purposes considered as being truly unpredictable and random. Such a generator, and associated method, are the subject of this patent.

Main problems associated with hardware random bit generators are **statistical bias** and **correlations among bits**. For completely random sequences of bits both statistical bias and correlations tend to zero, when the length of the sequence goes to infinity.

Quite generally, existing inventions suffer from a lack of a mathematical or scientific proof that, at least in some limit, both of the the following statements hold:

1. A generator provides, at its output (or outputs), low and high states (which are designated with "0" and "1" respectively) with probabilities $p(0)$ and $p(1)$ respectively such that $p(0) = p(1) = 0.5$. This is known as the "zero bias condition", with bias being defined as $\varepsilon = p(1) - 0.5$;
2. The low and high states, at the output (or outputs) of the generator make up a random, unpredictable sequence of bits.

The generator described here solves this problem. Namely, under some weak assumptions that can be easily met in practice, it is possible to prove mathematically that the principle of operation of the generator satisfies both aforementioned requirements and therefore produces truly random bits.

3 BACKGROUND OF THE INVENTION

Electronics circuits for generating random bits (or numbers) are well-known in the art They typically have one or more outputs which can take on either low ("0") or high ("1") digital level.

Electronic random bit (or number) generators fall into two large categories: pseudo-random generators and non-pseudo-random generators.

Pseudo-random generators

Pseudo-random generators are characterized by their ability to accept an initial state (or number) called the "seed" which completely determines the sequence of numbers that are produced by the generator thereof. Pseudo-random generators make use of a mathematical formula to "calculate" the numbers. Pseudo-random generators have a finite period, meaning that after a certain number of bits have been produced by the generator, it starts to produce the same sequence all over again. The length of the period may dramatically depend on a seed value. Some seed values are "strong" meaning they lead to a long repetition cycle for a given generator, others may be "weak" meaning that they lead to short repetition cycle and/or sequences with a bad statistical properties.

Moreover, some of the most popular pseudo-random generators are now known to produce numbers that have non desirable statistical properties (defects). Best modern pseudo-random generators seem to have no known statistical defects, but it seem obvious that numbers produced by a mathematical formula can not be truly random.

The idea behind pseudo-random generators is that to somebody who doesn't know the seed, produced sequence of bits looks like random in spite the fact that the whole sequence is determined by a formula. Actually, two generators of the same kind will produce exactly the same sequence of bits if fed by the same initial seed. This is called "synchronization of generators".

The possibility to synchronize pseudo-random generators is particularly useful for cryptographic purposes. In a most simplistic version, the seed serves as a secret key (or a password) and the sequence of bits produced by this seed is used as the one-time XOR pad. However, at the same time, this property of unique correspondence between the seed and the sequence of bits produced by the generator is a weakness, because a detailed knowledge about the generator's operating principle (and possible statistical defects) could help to reveal the key and/or break the encrypted code.

Non-pseudo-random generators

As opposed to pseudo-random generators, non-pseudo-random generators (or simply "hardware random bit generators") generators can not accept a seed. Such generators can not accept a seed and they have no initial state. They do not operate on a deterministic principle which would allow two generators to be synchronized. This impossibility of synchronization is their most important feature. It is particularly important for some applications like some newly developed cryptographic protocols which, by taking advantage of the "uniqueness" of the produced strings of bits, offer unconditional security. Under assumption that a generator produces truly random bits, no knowledge about its structure or operation principles can help a bit to predict its sequence and thus consequently to brake the encrypted code.

Random bit (or random number) hardware generators are relatively well-known in the patent literature. By their principle of operation they mainly fall in three classes discussed below.

The first class of generators works on the principle of a shift register with a feedback and a stochastic disturbance from the environment. That idea originates from the very famous principle used to generate pseudo-random numbers in hardware and software. The idea here is that a pseudo-random generator gets either re-seeded from time to time (or continually) with a seed that is gotten somehow from the random events gathered from the environment or to affect the feedback and thus destroy the predictability inherent to pseudo-random generators. However, known bad statistical properties of shift registers as random number generators may be inherited by this class of generators. There is also a potential problem of existence of "weak" and "strong" seeds that is necessarily brought up in this "blind seeding" approach. Examples of patented generators based on shift registers with a feedback and random disturbance form the environment are (Hofverberg 1995, Rostoker et. al. 1997).

The second class of generators uses the principle of sampling of fast ring oscillators or voltage-controlled oscillators, which sampling is done under control of (or in synchronization with) a slow oscillator. Namely, albeit digital, free-running ring oscillators suffer from catastrophic frequency instability which is caused by the minor temperature changes and/or noise that are normally present in electronics circuitry. Sampling the state of a fast ring oscillator is equivalent to stopping the spinning jack-pot wheel. Said fast voltage-controlled oscillator(s) may work in the chaotic regime (Bernstein et. al. 1991) or be controlled by the feedback signal from the output (Domenik et. al. 1987) or to oscillate freely without any feedback (Tanagawa 1992). Frequency of the slow oscillator may be additionally voltage-controlled with the analog noise (Hoffman 1998). Some inventions use several ring oscillators, coupled ring oscillators in the chaotic regime or other modifications of the basic principle. This approach contains in itself a danger of appearance of "remnants" of periodicity that is of course present in the ring oscillators. On top of that, these generators suffer form an unavoidable bias ($\varepsilon \neq 0$) that authors try to eliminate in various ways.

The third class of generators uses principle of sampling of digitized analog (white) noise source, which sampling is done under control of (or in synchronization with) a slow periodic oscillator, where the sampled bits serve either to directly produce random bits (Hoffmann 1978, Glazer 1985, Brown et. al. 1989, Dias 1989) or to choose between predetermined set of numbers (Hong et. al. 1997) or to measure the time intervals between like-polarity periods of the digitized noise (Simmons 1980). The main problems here are appearance of an unavoidable bias ($\varepsilon \neq 0$) and possible non-ideal statistical properties of random bits due to the finite bandwidth of the noise or a bad choice of digitalization procedure.

Quite generally, existing inventions in all three classes suffer from a lack of a mathematical or scientific proof that, at least in some limit, both of the requirements stated in the section TECHNICAL PROBLEM are fulfilled.

Invention presented here falls in the third class of generators, namely the class of generators which use electronics noise as the source of randomness. It will be shown that this generator fulfills both of the requirements in the limit of slow sampling.

4 DETAILED DESCRIPTION OF THE PRESENT INVENTION

Hardware generator of random bits presented here incorporates a circuit which makes sure that in the limit of slow enough sampling (that is slow rate of producing output bits), generated random bits are mutually statistically independent and have very low bias. Consequently, series of bits produced by the generator pass all known statistical tests of randomness, such as entropy test, Chisquare test, bias test, serial autocorrelation test, spectral test, Maurer's Universal test (Maurer 1992, Coron et. al 1999), and a collection of stringent tests known as the Diehard battery of tests (Marsaglia 1996).

Referring to the FIG.1, the random bit generator consists of the following six blocks:

1. A source of electric noise (FIG.1.100);
2. a DC decoupling capacitor (FIG.1.101);
3. a high-pass filter and amplifier (FIG.1.102);
4. a digitizing circuit consisting of a comparator controlled with a rough automatic zero-bias correction circuitry (FIG.1.103);
5. a time summation circuit for precision zero-bias correction and randomness enhancement (FIG.1.104);
6. a sampling circuit which delivers a bit upon a request (FIG.1.105).

The role of each block will be discussed.

The noise source, FIG.1.100, may be of any sort like resistive (Johnson's noise), semiconductor noise diode, inversely polarized base-collector junction of a bipolar transistor etc. but preferably a Zener diode. One possible realization of a noise circuit, which makes use of a Zener diode, is shown in the FIG.1.100, where Z denotes the Zener diode. It is well known fact that a Zener diode operating in a reverse polarity and the current strength near the knee, can serve as a noise generator. For example, a 6.8 Volt commercial Zener diode can produce a noise fluctuation of an amplitude of 30 to 50 mV (peak to peak) with a mean frequency of zero crossings of the order of 10 MHz.

It is also well known that a Zener diode of a knee voltage of less than 6.2 V operates mainly in the Quantum Mechanical (tunneling) regime, while the diodes with the knee above that operate mainly in the micro plasma regime (Somlo 1975). Both regimes have ideal properties of unpredictability needed for a truly random noise voltage source.

The best temperature stability of the noise amplitude is also obtained in the Zener diodes with the knee voltage of approx. 6.2 V, because then the two regimes with opposite temperature coefficients are in equilibrium (Somlo 1975). The same condition is also optimal from the point of the long term stability although, as it will become clear later, the generator presented here is extremely insensitive to the long term fluctuations of the noise source.

Decoupling capacitor (FIG.1.101). The DC voltage across the resistor *R* cannot be very well controlled in a high volume production and is probably susceptible to a long term drift comparable to or even higher than the noise amplitude which could disrupt digitalization of the signal. It is therefore desirable to decouple the noise source, by means of the capacitor *C* (FIG.1.101), in order to block the DC component and extract only the AC component of the noise.

The capacitor C (FIG.1.101) in series with the output resistance R of the previous stage (FIG 1.100) and the effective input resistance R' of next stage (FIG 1.102) forms a major contribution to an unwanted "memory". The timely persistence of this memory τ is equal to the product of the capacitance C and sum of the resistances R and R', that is: $\tau = C(R + R')$. Voltage amplitudes of any two noise variations which happen within the period τ will be mutually correlated because of the electric charge in the capacitor C which had not time to discharge through the resistance in the system. Luckily, this "memory" effect dies off exponentially with the time distance between the two variations, thus one can conclude that any two variations that are distant enough in time can be considered as statistically independent. Nevertheless, the "memory" of the circuit limits frequency bandwidth of the noise and sets an absolute upper limit to the bit extraction rate from the generator, which limit is independent of the latter bit extraction method.

High-pass filter and amplifier (FIG.1.102). The high-pass filter/amplifier HP has the purpose of stopping the low frequencies present in the noise that would cause comparator COMP in the next block (FIG.1.103) to lock in a single state for a long time. Because of the method of sampling (explained in what follows) used in this invention, such a lock would be undesirable. The high-pass filter FIG.1.102 should be designed such that it maximizes the mean frequency at the output of the comparator COMP in FIG.1.103. Such optimization ensures the highest bit extraction rate, at the output of the generator. Due to the reasons that will become clear later, it is important that the mean frequency of the digital signal at the output of the comparator COMP be much higher than the frequency of sampling (extraction) of bits at the output of the generator. As will be described later, the sampling is done via the Request pin of the sampling block FIG.1.105. The high-pass filter may also perform any amplification of the noise necessary for good operation of the comparator COMP.

Digitizing circuit (FIG.1.103). In this block the analog noise signal gets converted into a digital signal in form of logical "0" and "1". The digitizing circuit consists of a comparator COMP controlled with a rough automatic zero-bias feedback control.

The negative input of the comparator COMP should be connected to an appropriate DC reference voltage V_r. That voltage is important for correct operation of the comparator. The positive input of the comparator COMP is connected to the output of the previous stage FIG.1.102., which supplies the filtered AC noise voltage. Between the two said inputs of the comparator (positive and negative) a small DC "offset" voltage can be induced by virtue of the resistor R_i and the control current I_c that flows through it.

As the final result, the positive input of the comparator "sees" the sum of the offset voltage and the noise voltage. Whenever the sum exceeds the reference voltage V_r, the output of the comparator goes into the high logical state "1", whereas when the sum goes below the V_r, the output goes into the low logical state "0". This is illustrated by the graphs FIG.2.a and FIG.2.b.

By setting the control current I_c a little lower or higher, the output of the comparator COMP spends respectively a little more or less time in the logical state "1".

At some strength of the control current I_c, one can achieve that the comparator COMP spends approximately equally much time in either of the logical states. In another words, the duty cycle of the comparator COMP would then be approximately 0.5, on average. If, for any reason, the duty cycle gets is changed, the feedback network in FIG.1.103 will respond by changing the control current I_c in such a way that the duty cycle of 0.5 will be restored. Already here, at the output of the comparator COMP there is an approximately equal chance that the state is logical at "0" or at logical "1", that is the bias of the sampled output would be close to zero ($\varepsilon \approx 0$). But due to technical reasons it is quite difficult to keep the bias below 1/1000 (long term), and even this is possible only with addition of a precision potentiometer that would be used for a fine tuning of the referent voltage V_r.

Tuning the bias this way consumes a lot of time and would therefore be unfavorable for a mass production of the generator and miniaturization. Present invention eliminates the need to tune the bias to zero value, and actually allows to choose bias as low as desired, without the need to do any modifications to the circuit. This is made possible by means of a special circuit for timely summation. As the result, the generator needs no adjustments whatsoever and could be built on a single chip thus allowing for miniaturization.

The time summation block (FIG.1.104) is the crucial point of this invention. Namely, the JK-type flip-flop performs a continued summation of bits at its CP input, as will be explained. The result of the summation appears at the output Q of the said JK flip-flop and represents a new random bit sequence with highly suppressed bias and autocorrelation. To understand how this works it is important to bare in mind that the output Q of the said JK flip-flop is **sampled periodically** in time. This is a condition for a good operation of this generator. Said sampling is done by the next stage shown in FIG.1.105.

Without the loss of generality, let us suppose that at the time zero ($t = 0$) the Zener diode Z exhibits a voltage breakdown. (Voltage breakdown is only one of the processes that may cause fluctuations of the voltage across the diode that are manifested as noise. But to simplify the language we will refer to "voltage breakdown" as a synonym for a sudden positive jump of the voltage across the Zener diode.) This causes the output of the comparator COMP (FIG.1.103) to exhibit a positive going transition (and later a negative one). Every such event triggers the comparator COMP (FIG 1.103) thus causing the JK flip-flop (FIG.1.104) to reverse its state at the output Q. This is illustrated by the graphs FIG.2.b and FIG.2.c. The method that is the subject of this invention consists in sampling of the output Q of the said JK flip-flop periodically, at times $t = \Delta t$, $2\Delta t$, $3\Delta t$, ... and generally at times $t = i \times \Delta t$, where $i = 1, 2, 3, \ldots$. (Said sampling is performed by virtue of a D-type flip-flop described in the next block.) Let us suppose that the voltage breakdowns happen at times $t_0 = 0$, t_1, t_2, t_3, t_4, etc. At that moments, as explained, the JK flip-flop FIG.1.104 inverts its state at the output Q. Tiny intervals of time between neighboring voltage breakdowns $\Delta t_k = t_k - t_{k-1}$ where $k = 1, 2, 3, \ldots$ are distributed

according to some statistical distribution. The mean value μ of duration of this tiny intervals is defined as:

$$\mu = \lim_{N \to \infty} \frac{1}{N} \sum_{k=1}^{N} t_k \qquad (1)$$

For example, in the the pure Quantum Mechanical regime of the Zener diode, intervals between neighboring voltage breakdowns Δt_k follow the *Exponential* distribution. Mixing of the Quantum Mechanical model with the plasma noise, noise sources other than a diode or other models including effective memory and/or filtering of the noise signal prior to digitization, may lead to more centered distributions such as *Poisson* or even *Uniform* distribution. The power of this method is that the **knowledge of the actual distribution of the time intervals between neighboring voltage breakdowns is irrelevant.** It is only important that is *some* distribution and that its shape stays stable over a period of time substantially larger than the sampling period Δt.

Let us now suppose that the sampling period Δt is chosen large enough so that many voltage breakdowns happen during each sampling period. In another words, we suppose:

$$\Delta t >> \mu. \qquad (2)$$

This situation is illustrated in the FIG 2. where several voltage breakdowns in the noise signal (FIG.2.a) happen during any sampling period (FIG 2.d).

Furthermore, let us suppose that the said JK flip-flop (FIG.1.104) changes its state at the Q output: N_0 times from $t = 0$ till $t = \Delta t$, N_1 times from $t = \Delta t$ till $t = 2\Delta t$, and generally N_i times from $t = i\,\Delta t$, till $t = (i + 1)\Delta t$, where $i = 1, 2, 3, \ldots$.

Now we can conclude that every period of time Δt approximately equals the sum of many tiny intervals Δt_k:

$$\Delta t = \sum_{k=1}^{N_0} \Delta t_k$$
$$\Delta t = \sum_{k=N_0+1}^{N_0+N_1} \Delta t_k \qquad (3)$$

etc.

The above equalities hold only approximately because the first and last of the small intervals in a given sum may be only partially happening during the respective sampling period Δt. In such a case, a part of the first tiny interval may have actually happened during the previous period, while a part of the the last tiny interval may have actually happened during the next period (sum). However, approximation can be made arbitrarily good by taking large enough sampling period Δt.

The Central limit theorem of the Statistics states that the sum of a large number (say N) of independent random variables (for example Δt_k), which follow some (any) distribution, approaches *Normal* distribution in the limit of large N ($N \rightarrow \infty$). This means that the statistical variable x defined as:

$$x = \sum_{k=1}^{N} \Delta t_k \qquad (4)$$

follows approximately the *Normal* distribution, for large N. However, in our case defined by equations **(3)**, the "variable" x is fixed (being just Δt), and the relevant statistical random variable becomes the number of summands, N. In a special case, that is mentioned above, when the tiny intervals Δt_k are distributed according to the *Exponential* distribution, random variable N follows, by definition, exactly the *Poisson* distribution:

$$P(N) = \frac{(\Delta t/\mu)^N}{N!}\exp(-(\Delta t/\mu)). \qquad (5)$$

Quite generally, regardless of the distribution function of tiny intervals Δt_k it can be shown (Stipcevic) that the integer random variable N is distributed according to the *Binomial* distribution $B(N; 2\Delta t/\mu, p)$, where p is quickly approaching 0.5 as $\Delta t/\mu$ tends to infinity. Given the general expression for the *Binomial* distribution:

$$B(r;n,p) = \binom{n}{r} p^r (1-p)^{n-r} \qquad (6)$$

the distribution of the variable N can be written as:

$$B(N;2\Delta t/\mu, p) = \binom{2\Delta t/\mu}{N} p^N (1-p)^{2\Delta t/\mu - N} . \qquad (7)$$

This is not in contradiction with the previous result because the *Poisson* distribution (5) becomes equal to the *Binomial* distribution (7) in the limit $\Delta t/\mu \to \infty$.

It can be shown (Stipcevic) that as a special consequence of (7) the probability that the random variable N is **even** becomes equal to the probability that it is **odd**., in the limit $\Delta t/\mu \to \infty$.

But, when the JK flip-flop FIG.1.104. changes its state an even number of times its output Q returns to the initial state, say "0", whereas when it changes an odd number of times the output returns "1". Thus the probability of getting "0" would be equal to the probability of getting "1" at the output Sample (FIG.1.105), in the limit of slow sampling. This fact can be expressed like this:

$$\Delta t/\mu \to \infty \;\Rightarrow\; \varepsilon \to 0. \qquad (8)$$

Thus it is proved that the generator and corresponding method of sampling random phenomena **fulfill the first requirement** form the section TECHNICAL PROBLEM. This requirement is stating that the bias must vanish in some limit. The limit found here is that the sampling period Δt is much larger than the mean breakdown period μ.

The second requirement which states the statistical independence of the logical states (bits) at the output of the generator, is proved as follows. First we realize that the subsequent voltage breakdowns in the Zener diode are statistically independent because the breakdown itself is an unpredictable physical phenomenon. Secondly, the internal capacitive memory that appears in the circuit (which for example may be introduced by imperfections in electronics design, or be a part of physical process governing the alternate current noise source) "dies off" exponentially with the half-life τ. Effect of the memory on correlations can be made as small as desired in the limit of slow sampling, that is by making $\Delta t/\tau$ large enough. Namely, in the limit $\Delta t \,/\, \tau \rightarrow \infty$ sums of the type **(3)** are becoming mutually statistically independent. The statistical independence of two subsequent sums, in that limit, takes place because the two sums contain large portion of summands that are "out of the range" of the memory effect of each other. If we consider two sums that are not subsequent, then the memory effects are even smaller. This means that a bit corresponding to a sum becomes statistically independent of neighboring and even more all other bits, in the limit of slow sampling. Conclusion from this is that the generator and corresponding method of sampling random phenomena also **fulfill the second requirement** form the section TECHNICAL PROBLEM.

Finally **the sampling stage (FIG. 1.105)** consists of a D-type flip-flop which samples instantly the output of the JK flip-flop (FIG.1.104). Namely, when a positive-going edge of the sampling signal (that is transition from "0" to "1") appears at the input Request, state that is present at the input D gets sampled. Sampled value is memorized (frozen) and displayed at the output Q of the said D flip flop, and stays there until a new positive-going edge appears. By the definition of the D-type flip-flop, the sampling is done in a very short

instant of time so the output of the said flip-flop stays frozen for almost the whole sampling period Δt which makes possible for other devices (such as a computer) to read the generator's output safely. Functioning of this stage can be best understood by looking at the whole sequence of signals as shown in the FIG.2.

One can see that with each positive-going edge at the output of the comparator COMP (FIG.2.b), the JK flip-flop changes state at its Q output (FIG.2.c). The sampling signal (FIG.2.d) isn't, of course, in any synchronization with these signals, but whenever it exhibits a positive-going transition, the output Q of the JK flip-flop gets sampled and that value is the output bit from the generator (FIG.2.e).

It is important to notice that the output Q of the JK flip-flop FIG.1.104 by itself does not necessarily provide good quality random bits. However, sampling of the said output by the D-type flip-flop (FIG.1.105) provides a good quality random bits, in the limit of slow sampling ($\Delta t/\mu \to \infty$ and $\Delta t/\tau \to \infty$).

Results of the Monte Carlo simulation of the generator and the associated sampling method

Since in practice parameters μ and τ may be unknown, what is really a "large enough sampling period", Δt, is determined by an experimental method. Method consists of producing (by the generator in question) a set of long series of bits using different sampling periods and subjecting these series to statistical tests of randomness. Results of tests will reveal the minimum value of the sampling period at which produced bits pass all the tests. The generator should be used with that minimal or bigger sampling period.

As a simple example of an experimental method of finding out the minimal sampling period, but also as a confirmation that the method described in this invention works, we present here results of a computer Monte Carlo simulation of a generator based upon this method.

Simulation is based on a simulation of the tiny small voltage breakdown intervals Δt_k and follows exactly the principle of the block diagram of the sampling part FIG.1.104 and FIG.1.105, without any mathematical approximations. The simulations are made for two scenarios of statistical distributions of the time intervals Δt_k: *Exponential* and *Uniform*. The two distributions represent, in a way, the extreme cases: *Exponential* distribution is very asymmetric and has a long right-wing tail, while *Uniform* is totally symmetric and has no tails. There is a big chance that a realistic distribution some noise source would be somewhere between these two extremes. There are two benchmarks of the quality of bits simulated in this way: the bias ε (defined before) and the serial correlation coefficient a as defined in (Knuth 1997). Favorable value of the sampling period is indicated by both values being equal to zero within the statistical errors. The simulation does not include the memory effects of the hardware. Results of the simulation are displayed in the table below.

	Exponential distribution		*Uniform* distribution	
$\Delta t / \mu$	ε (± 0.00020)	a (± 0.00040)	ε (± 0.00020)	a (± 0.00040)
2.0	-0.00026	-0.32578	-0.00005	-0.05669
3.0	0.00005	-0.11039	0.00030	0.06362
4.0	-0.00002	-0.03845	0.00002	-0.03146
6.0	0.00008	-0.00495	-0.00004	0.00333
12.0	0.00001	0.00007	-0.00019	0.00008

In each simulation 6 250 000 bits were generated, which sets the size of errors with which the bias and serial autocorrelation were determined. The one sigma error on ε is 0.0002, and the one sigma error on a is 0.0004.

We see that already for the ratio of $\Delta t/\mu \geq 3$ the bias ε is equal to zero within the error for both distributions. This means that this method strongly suppresses the bias.

Behavior of the serial autocorrelation coefficient a is as expected: the coefficient becomes smaller as *sampling* goes slower. Note that the coefficient a tends more quickly to zero for *Uniform* distribution. This is because the *Uniform* distribution is symmetric (as opposed to very asymmetric *Exponential* distribution) this variable N in the equations (4) converges more quickly to the *Binomial* distribution, which is also symmetric.

Conclusion from these simulations is that the method which is the subject of this invention works and that is enough to sample bits 12 (or more) times lower frequency from the mean frequency of the noise in order to have a very high quality of random bits at the output of the generator. These simulations did not include effects of memory which may make the required ratio higher.

5 DESCRIPTION OF DRAWINGS

FIG. 1. - Block diagram of the random bit generator;

FIG. 2. - a) The noise signal;
b) the signal at the output of the comparator COMP in FIG.1.103;
c) the signal at the output Q of the JK flip-flop in FIG.1.104;
d) the sampling signal at the input of the D flip-flop in FIG.1.105;
e) logical output of the generator (bits).

FIG. 3. - A practical realization of the random bit generator with a Zener diode noise source.

6 DETAILED DESCRIPTION OF AT LEAST ONE PRACTICAL REALIZATION OF THE INVENTION

The drawing FIG.3 shows an example of possible schematic diagram of apparatus for generating true random bits based on time integration of a noise source realized with a semiconductor Zener diode. The diagram exploits the described sampling method and follows, in an obvious way, the structure of the block diagram in FIG.1. Zener diode Z is biased by a small inversely polarized current. The noise voltage appears across the resistor **R** (this refers to the block FIG.1.100). AC component of that current is distilled through the capacitor **C** and is fed to the operational amplifier **HP**. The capacitor **C** and resistors denoted by **R**, **R'** and $\mathbf{R_1}$ make a high-pass filter of gain 10 for the high frequencies (this corresponds to blocks FIG.1.101 and FIG.1.102). The noise so amplified and filtered i fed to the input of the comparator **COMP**, which together with the amplifier **OPA** makes up the digitizing circuit with the automatic zero-bias compensation (described in the block FIG.1.103). The remaining two flip-flops correspond in an obvious way to the blocks FIG.1.104 and FIG.1.105. On the schematic diagram FIG.3 there is added a circuit for conditioning the quality of the sampling clock signal at the **Request** input, which circuit consists of two Schmit triggers.

7 POSSIBLE APPLICATIONS OF THE INVENTION

Primary purpose of this invention is in products related to computers, cryptography and Internet, such as: peripheral generators of random numbers which may be connected to a computer via serial, parallel, IRDA, USB or some other port, PC cards including video controllers, cards for special purposes and PCMCIA cards, chips for generating random numbers intended for integration onto computer motherboards and other computer parts, Smart Cards, products for cryptographicaly secured communication, products for secure payment and business (B2C and B2B products) etc. The generator may also be used as an

analog noise source for electronics measurement equipment. The generator may also be used as a random number generator in hazard games automata.

8 BIBLIOGRAPHY

US 3,706,941	Dec. 19, 1972	Cohn, et. al.	331/078
US 3,790,768	Feb. 05, 1974	Chevalier, et. al	364/717
US 4,176,399	Apr. 21, 1978	Hoffmann	364/717
US 4,183,088	Jan. 8, 1980	Simmons	331/78
US 4,513,386	Apr. 23, 1985	Glazer	364/717
US 4,694,412	Sep. 15, 1987	Domenik, et. al.	364/717
US 4,810,975	Mar. 7, 1989	Dias	331/78
US 4,855,690	Aug. 8, 1989	Dias	331/78
US 4,853,884	Aug. 1, 1989	Brown, et. al.	364/602
US 5,007,087	Apr. 9, 1991	Bernstein, et. al.	380/28
US 5,117,380	May. 26, 1992	Tanagawa	364/717
US 5,434,806	Jul. 18, 1995	Hofverberg	364/717
US 5,625,825	Apr. 29, 1997	Rostoker, et. al.	395/325
US 5,627,775	May. 6, 1997	Hong, et. al.	364/717
US 5,706,218	Jan. 6, 1998	Hoffman	331/78
US 5,961,577	Oct. 5, 1999	Soenen, et. al.	708/251

P. I. Somlo, Zener-diode noise generators, Electronics Letters, 11 (1975), 290-290

D. E. Knuth, The art of computer programming Vol 2., 3rd ed., Reading MA, Addison-Wesley, 1997.

M. Stipcevic, Some Properties of Inverted Distributions, to be published in Web archive: Cryptology ePrint Archive (http://eprint.iacr.org)

U. Maurer, A Universal Statistical Test for Random Bit Generators, Journal of Cryptology, 5 (1992) 89-105

J-S. Coron, D. Naccache, An accurate evaluation of Maurer's Universal test, private communication, 1999.

G. Marsaglia, Diehard battery of tests, URL: http://stat.fsu.edu/~geo/diehard.html, 1996.

9 CLAIMS

1. Method for obtaining random bits from random physical events, which method can be proved to enhance randomness and ensure low bias, **characterized by**, counting of said events and associating to each even event a value of "0" and to each odd event a value of "1", and that the two said values "0" and "1" are sampled at periodic time instances, and that sampled values thus obtained represent resulting random bits.

2. Apparatus for generating random bits according to the claim 1., **characterized by**, two flip-flops; one of which is JK-type and the other of D-type; in the circuit shown on the FIG.1.104 and FIG.1.105.

3. Apparatus for automatic regulation of bias of stochastic digital signal shown on the FIG.1.103, which ensures stable value of bias against the changes in characteristics of electronics components of which the apparatus is made due to aging and/or temperature variations and/or supply voltage variations, **characterized by**, a negative feedback circuit which ensures that the output of the circuit spends approximately equal portion of time in the state of logical "1" as in the state of logical "0".

4. Apparatus for generating random bits according to the claim 1, **characterized by**, at least one apparatus described by claims 2 or 3.

5. Apparatus according to the claim 2 or 4, which generates at its output or outputs a sequence of unpredictable bits, **characterized by**, the fact that in the case all of the technical and methodological details about the apparatus are known it still would not be possible to sinchronize two or more such physically and methodologically identical generators to produce identical sequences of bits.

6. Use of the apparatus defined by any of the claims 2-5 which is based on the method described in claim 1, **characterized by**, a creation of sequence of random bits.

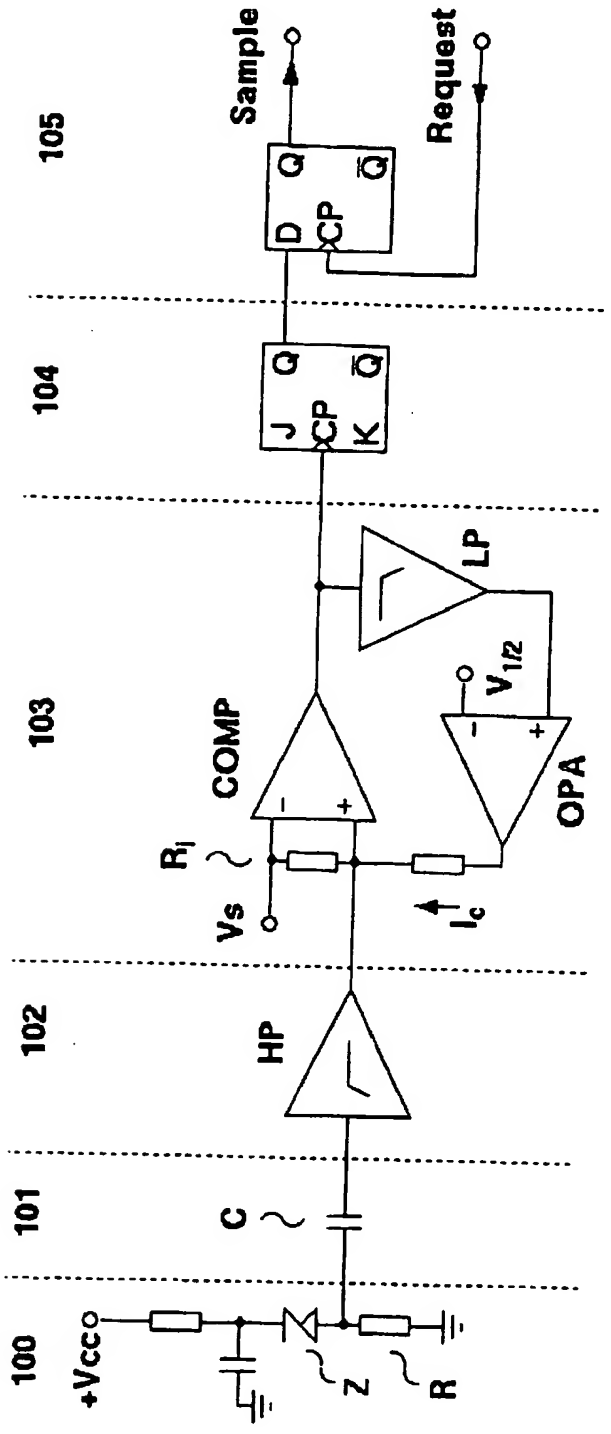
105
Sample
Request
Q
Q̄
D
CP
104
Q
Q̄
J
CP
K
103
LP
$V_{1/2}$
COMP
OPA
R_l
Vs
I_c
102
HP
101
C
100
+Vcc
Z
R

FIG 1.

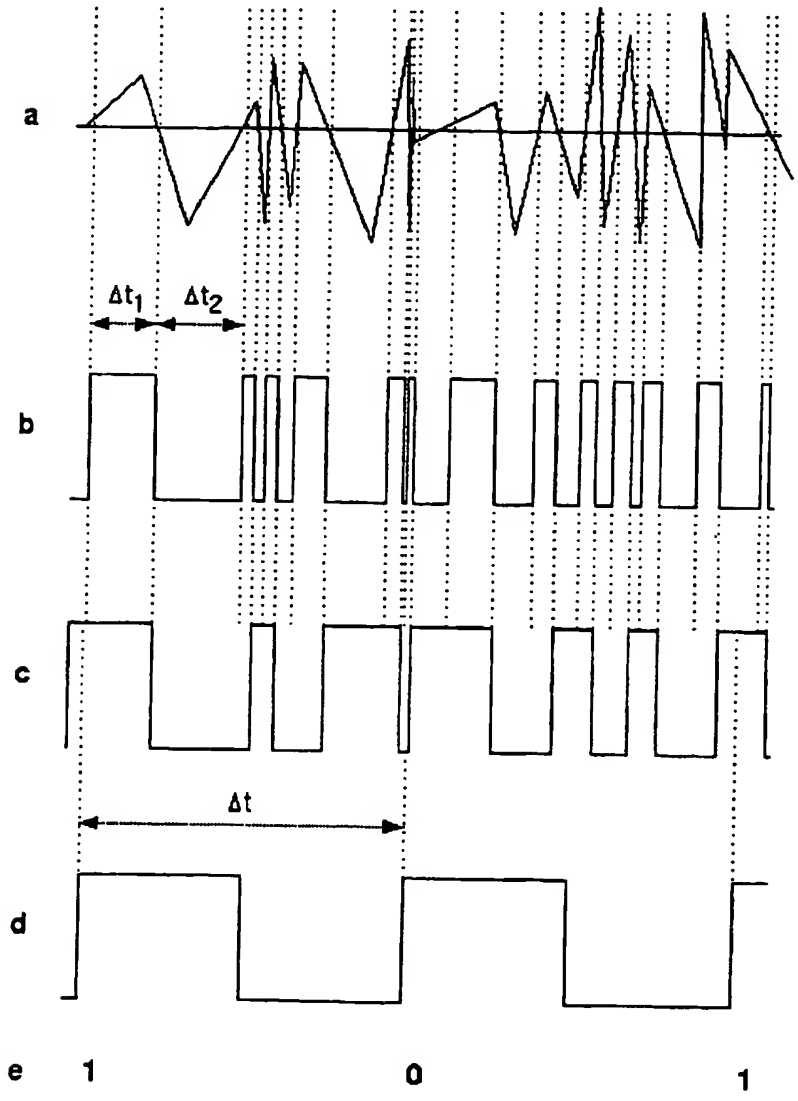

FIG.2

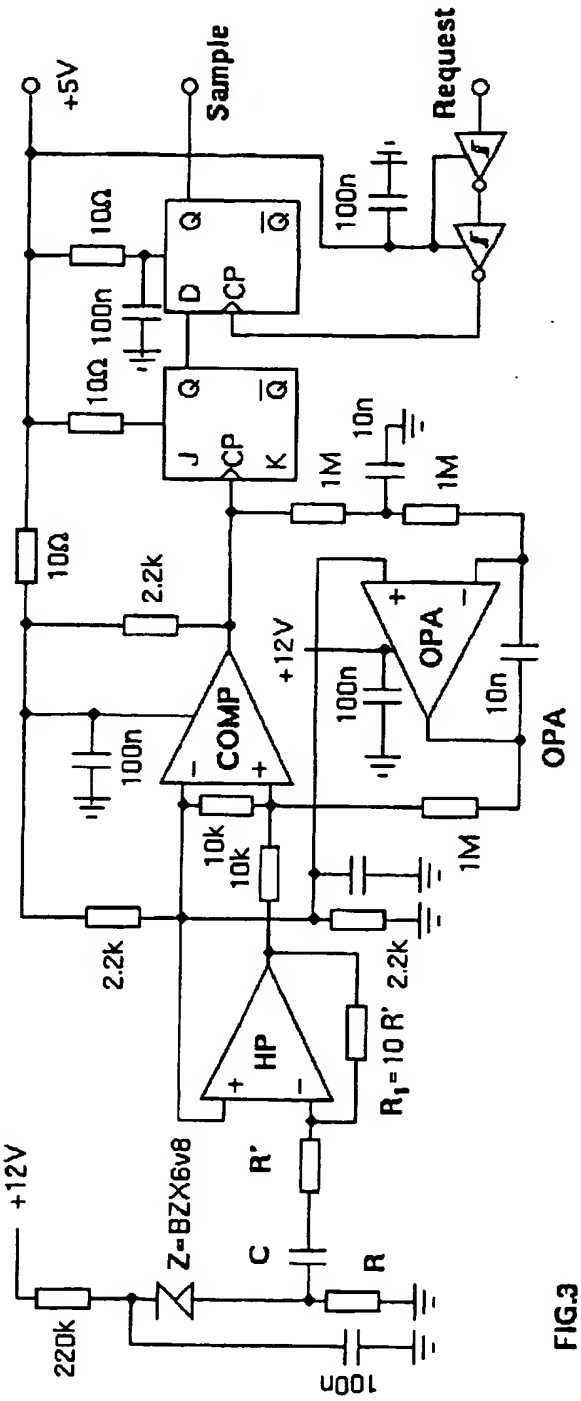
+5V
Sample
Request
10Ω
100n
Q
D
CP
J
K
1M
10n
2.2k
+12V
OPA
COMP
10k
HP
R'
C
R
Z=BZX6v8
220k
100n

FIG.3